

An Efficient Construction of Self-Dual Codes

Yoonjin Lee*

Department of Mathematics
Ewha Womans University
11-1 Daehyun-Dong, Seodaemun-Gu, Seoul
120-750, S. Korea
e-mail: yoonjinl@ewha.ac.kr

Jon-Lark Kim †

Department of Mathematics
328 Natural Sciences Building
University of Louisville
Louisville KY 40292 USA
e-mail: jl.kim@louisville.edu

Jan. 26, 2012

Abstract

We complete the building-up construction for self-dual codes by resolving the open cases over $GF(q)$ with $q \equiv 3 \pmod{4}$, and over \mathbb{Z}_{p^m} and Galois rings $GR(p^m, r)$ with an odd prime p satisfying $p \equiv 3 \pmod{4}$ with r odd. We also extend the building-up construction for self-dual codes to finite chain rings. Our building-up construction produces many new interesting self-dual codes. In particular, we construct 945 new extremal self-dual ternary $[32, 16, 9]$ codes, each of which has a trivial automorphism group. We also obtain many new self-dual codes over \mathbb{Z}_9 of lengths 12, 16, 20 all with minimum Hamming weight 6, which is the best possible minimum Hamming weight that free self-dual codes over \mathbb{Z}_9 of these lengths can attain. From the constructed codes over \mathbb{Z}_9 , we reconstruct optimal Type I lattices of dimensions 12, 16, 20, and 24 using Construction A; this shows that our building-up construction can make a good contribution for finding optimal Type I lattices as well as self-dual codes. We also find new optimal self-dual $[16, 8, 7]$ codes over $GF(7)$ and new self-dual codes over $GF(7)$ with the best known parameters $[24, 12, 9]$.

Key Words. building-up construction, self-dual code, chain ring, Galois ring.

*The author was supported by Priority Research Centers Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(2009-0093827).

†Corresponding author

1 Introduction

Self-dual codes have been of great interest because they often produce optimal codes and they also have beautiful connections to other mathematical areas including unimodular lattices, t -designs, Hadamard matrices, and quantum codes (see [39] for example).

There are several ways to construct self-dual codes. Early constructions are based on gluing vectors, which work well when the minimum distances of the codes are small (cf. [34, 36]). One powerful method is the balance principle [27, 32], which restricts the generator matrix of a self-dual code. Another general one is to build self-dual codes from self-dual codes of smaller lengths. The first such construction is based on shadow codes [4, 8]. M. Harada [18] introduced an easy way to generate many binary self-dual codes from a self-dual code of a smaller length, and then later the first author [29] introduced the so-called *building-up construction* for binary self-dual codes. This construction says that any binary self-dual code can be built from a self-dual code of smaller length. A few years later, the building-up construction for self-dual codes over finite fields $GF(q)$ was developed when q is a power of 2 or $q \equiv 1 \pmod{4}$ [30], and then over finite ring \mathbb{Z}_p^m with $p \equiv 1 \pmod{4}$ [33], and over Galois rings $GR(p^m, r)$ with $p \equiv 1 \pmod{4}$ with any r or $p \equiv 3 \pmod{4}$ with r even [31], where m is any positive integer. It turns out that the building-up construction is so efficient that one can easily find many (often new) self-dual codes of reasonable lengths (e.g., [14]).

In this paper, we complete the open cases of the building-up construction for self-dual codes over $GF(q)$ with $q \equiv 3 \pmod{4}$, and over \mathbb{Z}_p^m and Galois rings $GR(p^m, r)$ with an odd prime p such that $p \equiv 3 \pmod{4}$ with r odd. We also present a building-up construction for self-dual codes over finite chain rings.

Our building-up construction yields many new interesting self-dual codes. In fact, only one extremal self-dual ternary [32, 16, 9] code with a trivial automorphism group was known [20] before. In this paper, we construct 945 new extremal self-dual ternary [32, 16, 9] codes, each of which has a trivial automorphism group, i.e., the monomial group of order 2. We also obtain 208 new optimal self-dual [16, 8, 7] codes over $GF(7)$ and 59 new self-dual codes over $GF(7)$ with the best known parameters [24, 12, 9]. Furthermore, we construct many new self-dual codes over \mathbb{Z}_9 of lengths 12, 16, 20 all with minimum Hamming weight 6, which is the best possible minimum Hamming weight that free self-dual codes over \mathbb{Z}_9 of these lengths can have. From the self-dual codes over \mathbb{Z}_9 constructed by our building-up method, we reconstruct optimal Type I lattices of dimensions 12, 16, 20, and 24 using Construction A (refer to [3, 7, 11]). This shows that our building-up construction can make a good contribution for finding optimal Type I lattices as well as self-dual codes.

All our codes will be posted on www.math.louisville.edu/~jlkim/preprints.

2 Building-up construction for self-dual codes over $GF(q)$ with $q \equiv 3 \pmod{4}$

In this section we provide the building-up construction for self-dual codes over $GF(q)$ with $q \equiv 3 \pmod{4}$, where q is a power of an odd prime. It is known [39, p. 193] that if $q \equiv 3 \pmod{4}$ then a self-dual code of length n exists if and only if n is a multiple of 4. Our building-up construction needs the following known lemma [28, p. 281].

Lemma 2.1. *Let q be a power of an odd prime with $q \equiv 3 \pmod{4}$. Then there exist α and β in $GF(q)^*$ such that $\alpha^2 + \beta^2 + 1 = 0$ in $GF(q)$, where $GF(q)^*$ denotes the set of units of $GF(q)$.*

We give the *building-up construction* below and prove that it holds for any self-dual code over $GF(q)$ with $q \equiv 3 \pmod{4}$.

Proposition 2.2. *Let q be a power of an odd prime such that $q \equiv 3 \pmod{4}$, and let n be even. Let α and β be in $GF(q)^*$ such that $\alpha^2 + \beta^2 + 1 = 0$ in $GF(q)$. Let $G_0 = (\mathbf{r}_i)$ be a generator matrix (not necessarily in standard form) of a self-dual code \mathcal{C}_0 over $GF(q)$ of length $2n$, where \mathbf{r}_i are the row vectors for $1 \leq i \leq n$. Let \mathbf{x}_1 and \mathbf{x}_2 be vectors in $GF(q)^{2n}$ such that $\mathbf{x}_1 \cdot \mathbf{x}_2 = 0$ in $GF(q)$ and $\mathbf{x}_i \cdot \mathbf{x}_i = -1$ in $GF(q)$ for each $i = 1, 2$. For each i , $1 \leq i \leq n$, let $s_i := \mathbf{x}_1 \cdot \mathbf{r}_i$, $t_i := \mathbf{x}_2 \cdot \mathbf{r}_i$, and $\mathbf{y}_i := (-s_i, -t_i, -\alpha s_i - \beta t_i, -\beta s_i + \alpha t_i)$ be a vector of length 4. Then the following matrix*

$$G = \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & & & & \\ 0 & 1 & 0 & 0 & & & & \\ \hline & & \mathbf{y}_1 & & & \mathbf{r}_1 & & \\ & & \vdots & & & \vdots & & \\ & & \mathbf{y}_n & & & \mathbf{r}_n & & \end{array} \right]$$

generates a self-dual code \mathcal{C} over $GF(q)$ of length $2n + 4$.

Proof. We first show that any two rows of G are orthogonal to each other. Each of the first two rows of G is orthogonal to itself as the inner product of the i th row with itself equals $1 + \mathbf{x}_i \cdot \mathbf{x}_i = 0$ in $GF(q)$ for $i = 1, 2$. The first row of G is orthogonal to the second row of G as $\mathbf{x}_1 \cdot \mathbf{x}_2 = 0$ in $GF(q)$. Furthermore, the first row of G is orthogonal to any $(i + 2)$ th row of G for $1 \leq i \leq n$ since the inner product of the first row of G with the $(i + 2)$ th row of G is

$$(1, 0, 0, 0) \cdot \mathbf{y}_i + \mathbf{x}_1 \cdot \mathbf{r}_i = -s_i + s_i = 0.$$

Similarly, the second row of G is orthogonal to any $(i + 2)$ th row of G for $1 \leq i \leq n$. We note that $\mathbf{r}_i \cdot \mathbf{r}_j = 0$ for $1 \leq i, j \leq n$. Any $(i + 2)$ th row of G is orthogonal to any $(j + 2)$ th row for $1 \leq i, j \leq n$ because the inner product of the $(i + 2)$ th row of G with the $(j + 2)$ th row is equal to

$$\mathbf{y}_i \cdot \mathbf{y}_j + \mathbf{r}_i \cdot \mathbf{r}_j = (1 + \alpha^2 + \beta^2)(s_i s_j + t_i t_j) = 0 \quad \text{in } GF(q).$$

Therefore, \mathcal{C} is self-orthogonal; so $\mathcal{C} \subseteq \mathcal{C}^\perp$.

We claim that the code \mathcal{C} is of dimension $n + 2$. It suffices to show that no nontrivial linear combination of the first two rows of G is in the span of the bottom n rows of G . Assume such a combination exists. Then c_1 (the first row of G) + c_2 (the second row of G) = $\sum_{i=1}^n d_i(\mathbf{y}_i, \mathbf{r}_i)$ for some nonzero c_1 or c_2 in $GF(q)$ and some d_i in $GF(q)$ with $i = 1, \dots, n$. Then comparing the first four coordinates of the vectors in both sides, we get $c_1 = -\sum_{i=1}^n d_i s_i$, $c_2 = -\sum_{i=1}^n d_i t_i$, $0 = -\sum_{i=1}^n d_i(\alpha s_i + \beta t_i)$, $0 = \sum_{i=1}^n d_i(-\beta s_i + \alpha t_i)$; thus $0 = -\sum_{i=1}^n d_i(\alpha s_i + \beta t_i) = \alpha(-\sum_{i=1}^n d_i s_i) + \beta(-\sum_{i=1}^n d_i t_i) = \alpha c_1 + \beta c_2$, that is, we have $\alpha c_1 + \beta c_2 = 0$. Similarly we also have $-\beta c_1 + \alpha c_2 = 0$. From both equations $\alpha c_1 + \beta c_2 = 0$, $-\beta c_1 + \alpha c_2 = 0$, it follows that $c_1 = c_2 = 0$, a contradiction.

As the code \mathcal{C} is of dimension $n + 2$ and $\dim \mathcal{C} + \dim \mathcal{C}^\perp = 2n + 4$, \mathcal{C} and \mathcal{C}^\perp have the same dimension. Since $\mathcal{C} \subseteq \mathcal{C}^\perp$, we have $\mathcal{C} = \mathcal{C}^\perp$, that is, \mathcal{C} is self-dual. \square

We give a more efficient algorithm to construct G in Proposition 2.2 as follows. The idea of this construction comes from the recursive algorithm in [1], [2].

Modified building-up construction

- Step 1:

Under the same notations as above, we consider the following.

For each i , let s_i and t_i be in $GF(q)$ and define $\mathbf{y}_i := (s_i, t_i, \alpha s_i + \beta t_i, \beta s_i - \alpha t_i)$ be a vector of length 4. Then

$$G_1 = \left[\begin{array}{c|c} \mathbf{y}_1 & \mathbf{r}_1 \\ \vdots & \vdots \\ \mathbf{y}_n & \mathbf{r}_n \end{array} \right]$$

generates a self-orthogonal code C_1 .

- Step 2:

Let C be the dual of C_1 . Consider the quotient space C/C_1 . Let U_1 be the set of all coset representatives of the form $\mathbf{x}'_1 = (1 \ 0 \ 0 \ 0 \ \mathbf{x}_1)$ such that $\mathbf{x}'_1 \cdot \mathbf{x}'_1 = 0$ and U_2 the set of all coset representatives of the form $\mathbf{x}'_2 = (0 \ 1 \ 0 \ 0 \ \mathbf{x}_2)$ such that $\mathbf{x}'_2 \cdot \mathbf{x}'_2 = 0$.

- Step 3:

For any $\mathbf{x}'_1 \in U_1$ and $\mathbf{x}'_2 \in U_2$ such that $\mathbf{x}'_1 \cdot \mathbf{x}'_2 = 0$, the following matrix

$$G = \left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & \mathbf{x}_1 \\ 0 & 1 & 0 & 0 & \mathbf{x}_2 \\ \hline \mathbf{y}_1 & & & & \mathbf{r}_1 \\ \vdots & & & & \vdots \\ \mathbf{y}_n & & & & \mathbf{r}_n \end{array} \right]$$

generates a self-dual code \mathcal{C} over $GF(q)$ of length $2n + 4$.

Then, we have the following immediately.

Proposition 2.3. *Let SD_1 be the set of all self-dual codes obtained from Proposition 2.2 with all possible vectors of \mathbf{x}_1 and \mathbf{x}_2 . Let SD_2 be the set of all self-dual codes obtained from the modified building-up construction with all possible values of s_i and t_i in $GF(q)$ for $1 \leq i \leq n$. Then $SD_1 = SD_2$.*

What follows is the converse of Proposition 2.2, that is, every self-dual code over $GF(q)$ with $q \equiv 3 \pmod{4}$ can be obtained by the building-up method in Proposition 2.2.

Proposition 2.4. *Let q be a power of an odd prime such that $q \equiv 3 \pmod{4}$. Any self-dual code \mathcal{C} over $GF(q)$ of length $2n$ with even $n \geq 4$ is obtained from some self-dual code \mathcal{C}_0 over $GF(q)$ of length $2n - 4$ (up to permutation equivalence) by the construction method given in Proposition 2.2.*

Proof. Let G be a generator matrix of \mathcal{C} . Without loss of generality we may assume that $G = (I_n \mid A) = (\mathbf{e}_i \mid \mathbf{a}_i)$, where \mathbf{e}_i and \mathbf{a}_i are the row vectors of I_n (= the identity matrix) and A , respectively for $1 \leq i \leq n$. It is enough to show that there exist vectors $\mathbf{x}_1, \mathbf{x}_2$ in $GF(q)^{2n-4}$ and a self-dual code \mathcal{C}_0 over $GF(q)$ of length $2n - 4$ whose extended code \mathcal{C}_1 (constructed by the method in Proposition 2.2) is equivalent to \mathcal{C} .

We note that $\mathbf{a}_i \cdot \mathbf{a}_j = 0$ for $i \neq j$, $1 \leq i, j \leq n$ and $\mathbf{a}_i \cdot \mathbf{a}_i = -1$ for $1 \leq i \leq n$ since \mathcal{C} is self-dual. Let α and β be in $GF(q)^*$ such that $\alpha^2 + \beta^2 + 1 = 0$ in $GF(q)$. We notice that \mathcal{C} also has the following generator matrix

$$G' := \left[\begin{array}{ccc|ccc} \mathbf{e}_1 + \alpha\mathbf{e}_3 + \beta\mathbf{e}_4 & & & \mathbf{a}_1 + \alpha\mathbf{a}_3 + \beta\mathbf{a}_4 & & \\ \mathbf{e}_2 + \beta\mathbf{e}_3 - \alpha\mathbf{e}_4 & & & \mathbf{a}_2 + \beta\mathbf{a}_3 - \alpha\mathbf{a}_4 & & \\ & \mathbf{e}_3 & & & \mathbf{a}_3 & \\ & \mathbf{e}_4 & & & \mathbf{a}_4 & \\ & \vdots & & & \vdots & \\ & \mathbf{e}_n & & & \mathbf{a}_n & \end{array} \right].$$

Deleting the first four columns and the third and fourth rows of G' produces the following $(n - 2) \times (2n - 4)$ matrix G_0 :

$$G_0 := \left[\begin{array}{ccc|ccc} 0 & \cdots & 0 & \mathbf{a}_1 + \alpha\mathbf{a}_3 + \beta\mathbf{a}_4 & & \\ 0 & \cdots & 0 & \mathbf{a}_2 + \beta\mathbf{a}_3 - \alpha\mathbf{a}_4 & & \\ & & & \mathbf{a}_5 & & \\ & & & \vdots & & \\ & I_{n-4} & & \mathbf{a}_n & & \end{array} \right]$$

We claim that G_0 is a generator matrix of some self-dual code \mathcal{C}_0 of length $2n - 4$. We first show that G_0 generates a self-orthogonal code \mathcal{C}_0 as follows. The inner product of the first row of G_0 with itself is equal to

$$\mathbf{a}_1 \cdot \mathbf{a}_1 + \alpha^2 \mathbf{a}_3 \cdot \mathbf{a}_3 + \beta^2 \mathbf{a}_4 \cdot \mathbf{a}_4 = -(1 + \alpha^2 + \beta^2) = 0,$$

and similarly the second row is orthogonal to itself. For $3 \leq i \leq n-2$, the inner product of the i th row of G_0 with itself equals $1 + \mathbf{a}_{i+2} \cdot \mathbf{a}_{i+2} = 0$. The inner product of the first row of G_0 with the second row is $\alpha\beta\mathbf{a}_3 \cdot \mathbf{a}_3 - \alpha\beta\mathbf{a}_4 \cdot \mathbf{a}_4 = 0$. Clearly, for $1 \leq i, j \leq n-2$ with $i \neq j$, any i th row is orthogonal to any j th row.

Now we show that $|\mathcal{C}_0| = q^{n-2}$, so \mathcal{C}_0 is self-dual. First of all, we note that both vectors $\mathbf{v}_1 := \mathbf{a}_1 + \alpha\mathbf{a}_3 + \beta\mathbf{a}_4$ and $\mathbf{v}_2 := \mathbf{a}_2 + \beta\mathbf{a}_3 - \alpha\mathbf{a}_4$ in the first two rows of G_0 contain units. Otherwise, both vectors are zero vectors. Then $\mathbf{a}_1 = -(\alpha\mathbf{a}_3 + \beta\mathbf{a}_4)$, then $-1 = \mathbf{a}_1 \cdot \mathbf{a}_1 = (\alpha\mathbf{a}_3 + \beta\mathbf{a}_4) \cdot (\alpha\mathbf{a}_3 + \beta\mathbf{a}_4) = -(\alpha^2 + \beta^2) = 1$, i.e., $-1 = 1$ in $GF(q)$, which is impossible since q is odd. So, \mathbf{v}_1 is a nonzero vector, and hence it contains a unit. Similarly, it is also true for \mathbf{v}_2 . We can also show that \mathbf{v}_1 and \mathbf{v}_2 are linearly independent. If not, $\mathbf{v}_1 = c\mathbf{v}_2$ for some c in $GF(q)^*$. Then by taking inner products of both sides with \mathbf{a}_1 , we have $\mathbf{a}_1 \cdot \mathbf{v}_1 = c\mathbf{a}_1 \cdot \mathbf{v}_2$, so we get $-1 = 0$, a contradiction. Therefore it follows that G_0 is equivalent to a standard form of matrix $[I_{n-2} \mid *]$, so that $|\mathcal{C}_0| = q^{n-2}$, that is, \mathcal{C}_0 is self-dual.

Let $\mathbf{x}_1 = (0, \dots, 0 \mid \mathbf{a}_1)$ and $\mathbf{x}_2 = (0, \dots, 0 \mid \mathbf{a}_2)$ be row vectors of length $2n-4$. Then for $i = 1, 2$, $\mathbf{x}_i \cdot \mathbf{x}_i = \mathbf{a}_i \cdot \mathbf{a}_i = -1$ in $GF(q)$ and $\mathbf{x}_1 \cdot \mathbf{x}_2 = \mathbf{a}_1 \cdot \mathbf{a}_2 = 0$ in $GF(q)$. Using the vectors $\mathbf{x}_1, \mathbf{x}_2$ and the self-dual code \mathcal{C}_0 , we can construct a self-dual code \mathcal{C}_1 with the following $n \times 2n$ generator matrix G_1 by Proposition 2.2:

$$G_1 := \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & \cdots & 0 & \mathbf{a}_1 \\ 0 & 1 & 0 & 0 & 0 & \cdots & 0 & \mathbf{a}_2 \\ \hline 1 & 0 & \alpha & \beta & 0 & \cdots & 0 & \mathbf{a}_1 + \alpha\mathbf{a}_3 + \beta\mathbf{a}_4 \\ 0 & 1 & \beta & -\alpha & 0 & \cdots & 0 & \mathbf{a}_2 + \beta\mathbf{a}_3 - \alpha\mathbf{a}_4 \\ 0 & 0 & 0 & 0 & & & & \mathbf{a}_5 \\ \vdots & \vdots & \vdots & \vdots & & & & \vdots \\ 0 & 0 & 0 & 0 & I_{n-4} & & & \mathbf{a}_n \end{array} \right]$$

Clearly G_1 is row equivalent to G . Hence the given code \mathcal{C} is the same as the code \mathcal{C}_1 that is obtained from the code \mathcal{C}_0 by the building-up construction in Proposition 2.2. This completes the proof. \square

Remark 2.5. Note that in the statement of Proposition 2.4 we do not have any condition on the minimum distance of \mathcal{C} . In the middle part of the proof of Proposition 2.4 we have shown that G_0 has size $(n-2) \times (2n-4)$ and has dimension $n-2$ without using the minimum distance of \mathcal{C} .

2.1 Self-dual codes over $GF(3)$

We consider self-dual codes over $GF(3)$. The classification of extremal self-dual codes over $GF(3)$ was known up to length 24. For length $n = 28$, only 32 ternary extremal self-dual codes were known [25], [19] (or see [26]). In particular, W. C. Huffman [25] classified all $[28, 14, 9]$ self-dual ternary codes with a monomial automorphism of prime order ≥ 5 and showed that there are exactly 19 such codes. Using Proposition 2.2 with the Pless symmetry code $\mathcal{S}(11)$ of length 24 (see [37], [27]), we find easily at least 673 inequivalent $[28, 14, 9]$

Table 1: Ternary $[28, 14, 9]$ self-dual codes using $\mathcal{S}(11)$ with $\mathbf{x}_1 = (000000000021212121000000)$

Code No.	$\mathbf{x}_2 = (0 \dots 0x_{11} \dots x_{24})$	$ \text{Aut} $
1	0 1 2 2 2 2 1 0 2 1 0 0 0 0	2
2	1 0 2 1 1 1 1 0 2 1 0 0 0 0	2
3	2 2 1 0 1 1 2 0 2 1 0 0 0 0	2
4	1 2 1 0 2 1 2 0 2 1 0 0 0 0	2
5	2 0 0 2 2 2 1 1 2 1 0 0 0 0	2
6	2 0 1 1 1 0 1 1 2 1 0 0 0 0	2
7	2 0 2 1 1 0 1 2 2 1 0 0 0 0	2
8	2 0 1 1 2 0 1 2 2 1 0 0 0 0	4
9	0 1 1 1 2 0 1 2 2 1 0 0 0 0	2
10	1 0 2 1 2 0 1 2 2 1 0 0 0 0	2
11	1 0 0 1 1 1 2 2 2 1 0 0 0 0	4
12	1 2 0 0 2 1 2 2 2 1 0 0 0 0	2
13	0 1 1 2 2 2 0 1 1 1 0 0 0 0	2
14	1 0 2 2 2 2 0 1 1 1 0 0 0 0	2
15	0 1 2 2 2 0 1 2 1 1 0 0 0 0	2
16	1 2 1 0 2 1 2 0 1 1 0 0 0 0	2
17	2 1 1 0 2 2 1 0 0 2 1 0 0 0	2
18	2 2 2 0 2 2 1 0 0 2 1 0 0 0	4
19	1 1 2 0 2 2 1 0 0 2 1 0 0 0	4
20	0 0 1 0 2 2 1 2 2 2 0 1 0 0	8

self-dual ternary codes whose full automorphism group order is 2^{i+1} , $i = 0, 1, 2$. Note that any ternary code has a trivial automorphism of order 2. We list only 20 of them in order to save space in Table 1, where $\mathbf{x}_1 = (000000000021212121000000)$ and the 14 entries of the right side of \mathbf{x}_2 are displayed in the second column, and the order of the automorphism group of the corresponding code is given in the last column. We note that by Construction A (see [7], [22], or Section 3.3, for example) the corresponding lattice $\Lambda(C)$ of any ternary self-dual $[28, 14, 9]$ code C produces an optimal Type I 28-dimensional unimodular lattice with minimum norm 3. On the other hand, Harada, Munemasa and Venkov have recently verified that there are exactly 6,931 extremal self-dual codes over $GF(3)$ [23], using the classification of all the 28-dimensional unimodular lattices with minimum norm 3.

For length $n = 32$, Huffman [25] classified all ternary $[32, 16, 9]$ self-dual codes with a monomial automorphism of prime order $r \geq 5$. He showed that r can be assumed to be $r = 5$ or $r = 7$. More precisely, he showed that there are exactly 239 inequivalent extremal self-dual ternary $[32, 16, 9]$ codes with monomial automorphisms of prime order 5 and exactly 16 inequivalent extremal self-dual ternary $[32, 16, 9]$ codes with monomial automorphisms of prime order 7. The equivalence between these two classes of codes was not done. Only one extremal self-dual $[32, 16, 9]$ code with a trivial automorphism group

Table 2: New ternary $[32, 16, 9]$ self-dual codes with trivial automorphism groups using $G(C_{28})$ with $\mathbf{x}_1 = (0000000000002121212100000000)$

Code No.	$\mathbf{x}_2 = (0 \dots 0x_{13} \dots x_{28})$
1	1 2 1 1 2 1 0 0 2 1 0 0 0 0 0 0
2	1 1 1 2 2 1 0 0 2 1 0 0 0 0 0 0
3	2 2 1 2 2 1 0 0 2 1 0 0 0 0 0 0
4	2 2 1 1 1 1 0 0 2 1 0 0 0 0 0 0
5	1 1 1 1 1 1 0 0 2 1 0 0 0 0 0 0
6	1 2 2 1 1 1 0 0 2 1 0 0 0 0 0 0
7	2 2 2 2 1 1 0 0 2 1 0 0 0 0 0 0
8	1 1 2 1 1 2 0 0 2 1 0 0 0 0 0 0
9	2 2 2 1 1 2 0 0 2 1 0 0 0 0 0 0
10	1 1 2 2 2 2 0 0 2 1 0 0 0 0 0 0
11	2 2 2 2 2 2 0 0 2 1 0 0 0 0 0 0
12	1 1 1 1 2 2 0 0 2 1 0 0 0 0 0 0
13	2 2 1 1 2 2 0 0 2 1 0 0 0 0 0 0
14	1 2 2 1 2 2 0 0 2 1 0 0 0 0 0 0
15	1 1 2 1 0 2 1 0 2 1 0 0 0 0 0 0
16	2 2 2 1 0 2 1 0 2 1 0 0 0 0 0 0
17	0 1 2 1 1 2 1 0 2 1 0 0 0 0 0 0
18	1 1 0 1 2 2 1 0 2 1 0 0 0 0 0 0
19	0 1 1 1 2 2 1 0 2 1 0 0 0 0 0 0
20	0 1 2 2 2 2 1 0 2 1 0 0 0 0 0 0

was found in [20], but we have found a lot as shown below. Recently Harada et. al. [21] have found 53 more inequivalent extremal self-dual $[32, 16, 9]$ codes whose automorphism group orders are divisible by 32. Therefore the currently known number of inequivalent extremal self-dual ternary $[32, 16, 9]$ codes is 293 [21].

Using Proposition 2.2 with a ternary self-dual $[28, 14, 9]$ code C_{28} whose generator matrix $G(C_{28})$ is given below, we find at least 945 inequivalent $[32, 16, 9]$ self-dual ternary codes, each of which has a trivial automorphism group. These are not equivalent to the self-dual $[32, 16, 9]$ code with a trivial automorphism group in [20]. We have stopped running Magma [6] and expect that there will be more such codes. We list only 20 of them in order to save space in Table 2, where the 16 entries of the right side of \mathbf{x}_2 are displayed in the second column.

We summarize our result as follows.

Proposition 2.6. *There are at least 1238 inequivalent extremal ternary self-dual $[32, 16, 9]$ codes, 946 of which have trivial automorphism groups.*

$$G(\mathcal{C}_{28}) = \begin{bmatrix} 1000000000000021212121000000 \\ 0100000000000001222210210000 \\ 22101000000000001111111111 \\ 1011010000000000201211122212 \\ 0000001000000000220121112221 \\ 2101000100000000212012111222 \\ 1202000010000000221201211122 \\ 0112000001000000222120121112 \\ 2022000000100000222212012111 \\ 2101000000010000212221201211 \\ 0000000000001000211222120121 \\ 1120000000000100211122212012 \\ 0221000000000010221112221201 \\ 1120000000000001212111222120 \end{bmatrix}$$

2.2 Self-dual codes over $GF(7)$

Next we consider self-dual codes over $GF(7)$. The classification of self-dual codes over $GF(7)$ was known up to lengths 12 (see [12, 13, 24, 38]). The papers [12, 13] used the monomial equivalence and monomial automorphism groups of self-dual codes over $GF(7)$. Hence we also use the monomial equivalence and monomial automorphism groups. On the other hand, the $(1, -1, 0)$ -monomial equivalence was used in [38, Theorem 1] to give a mass formula:

$$\sum_j \frac{2^n n!}{|Aut(C_j)|} = N(n) = 2 \prod_{i=1}^{(n-2)/2} (7^i + 1),$$

where $N(n)$ denotes the total number of distinct self-dual codes over $GF(7)$. In particular, when $n = 16$, there are at least $785086 > N(16)/2^{16}16!$ inequivalent self-dual $[16, 8]$ codes over $GF(7)$ under the $(1, -1, 0)$ -monomial equivalence. It will be very difficult to classify all self-dual $[16, 8]$ codes. In what follows, we focus on self-dual codes with the highest minimum distance.

For length $n = 16$, only ten optimal self-dual $[16, 8, 7]$ codes over $GF(7)$ were known [13]. These have (monomial) automorphism group orders 96 or 192. We construct at least 214 self-dual $[16, 8, 7]$ codes over $GF(7)$ by applying the building-up construction to the bordered circulant code with $\alpha = 0, \beta = 2 = \gamma$ and the row $(2, 5, 5, 2, 0)$, denoted by $C_{1,1}$ in [12]. We check that the 207 codes of the 214 codes have automorphism group orders 6, 12, 24, 48, 72, and hence they are new. On the other hand, the remaining seven codes have group orders 96 or 192, and we have checked that six of them are equivalent to the first four codes and the last two codes in [13, Table 7], and that the remaining one code is new. We list 20 of our 214 codes in Table 3, where \mathbf{x}_1 and \mathbf{x}_2 are given in the second and third columns respectively,

Table 3: New $[16, 8, 7]$ self-dual codes over $GF(7)$ using $C_{1,1}$ in [12]

#	$\mathbf{x}_1 = (0 \dots 0x_1 \dots x_{12})$	$\mathbf{x}_2 = (0 \dots 0x_5 \dots x_{12})$	$ \text{Aut} $	A_7, A_8
1	2 1 2 6 1 6 1 0	1 2 1 1 6 5 1 0	24	696, 3432
2	1 2 2 6 1 6 1 0	4 5 6 4 4 6 1 0	24	720, 3360
3	5 1 5 6 1 6 1 0	4 5 1 3 6 1 3 0	12	636, 3780
4	5 1 5 1 1 6 1 0	6 3 3 6 1 2 3 0	6	564, 3996
5	6 5 5 1 1 6 1 0	3 4 1 2 4 1 1 0	12	540, 4068
6	5 2 1 1 1 6 1 0	2 1 2 1 5 2 3 0	12	588, 3924
7	1 6 2 2 1 6 1 0	3 2 1 5 1 2 2 0	6	612, 3804
8	4 2 3 3 1 6 1 0	3 3 5 3 3 5 2 0	12	576, 3936
9	5 3 3 3 1 6 1 0	4 1 4 5 1 3 1 0	12	588, 3876
10	3 2 4 3 1 6 1 0	5 5 2 4 1 5 1 0	12	552, 4104
11	2 3 4 3 1 6 1 0	4 4 5 4 4 2 2 0	12	624, 3744
12	5 4 4 3 1 6 1 0	3 6 2 6 3 1 3 0	12	612, 3852
13	5 3 4 4 1 6 1 0	5 5 5 3 5 1 1 0	48	576, 3936
14	1 5 1 5 1 6 1 0	3 1 1 2 4 3 1 0	24	480, 4320
15	2 6 1 5 1 6 1 0	5 3 1 1 1 3 3 0	24	672, 3552
16	3 4 4 5 1 6 1 0	5 2 5 3 6 2 1 0	48	528, 4128
17	2 1 6 5 1 6 1 0	6 2 5 2 3 2 1 0	12	672, 3552
18	5 2 3 5 2 6 1 0	1 4 4 5 1 4 1 0	12	660, 3708
19	2 2 4 5 2 6 1 0	2 1 2 1 2 5 3 0	6	564, 4092
20	6 6 6 5 2 6 1 0	1 3 1 4 6 2 3 0	6	600, 3912

and A_7 and A_8 are given in the last column so that the Hamming weight enumerator of the corresponding code can be derived from the appendix of [13].

Theorem 2.7. *There exist at least 218 self-dual $[16, 8, 7]$ codes over $GF(7)$.*

For length 20 only one optimal self-dual $[20, 10, 9]$ code over $GF(7)$ is known [12], [13]. It is an open question to determine whether this code is unique.

For length 24 there are 488 best known self-dual $[24, 12, 9]$ codes over $GF(7)$ [13]. It has been confirmed [17] that the 488 codes in [13] (only 40 codes are shown in [13]) have non-trivial automorphism groups. On the other hand, we have found at least 59 self-dual $[24, 12, 9]$ codes over $GF(7)$, each of which has a trivial automorphism group. To do this, we have used the bordered circulant code over $GF(7)$ with $\alpha = 2, \beta = 1 = \gamma$ and the row $(4, 6, 3, 6, 6, 1, 4, 3, 0)$, denoted by $C_{20,1}$ [12]. We list 10 of our 59 codes in Table 4, where \mathbf{x}_1 and \mathbf{x}_2 are given in the second and third columns respectively, and A_9, \dots, A_{12} are given in the last column so that the Hamming weight enumerator of the corresponding code can be derived from the appendix of [13]. We therefore obtain the following theorem.

Theorem 2.8. *There exist at least 547 self-dual $[24, 12, 9]$ codes over $GF(7)$.*

Table 4: New $[24, 12, 9]$ self-dual codes over $GF(7)$ using $C_{20,1}$ in [12] with trivial automorphism groups

#	$\mathbf{x}_1 = (0 \dots 0x_9 \dots x_{20})$	$\mathbf{x}_2 = (0 \dots 0x_9 \dots x_{20})$	$A_9, A_{10}, A_{11}, A_{12}$
1	2 6 2 3 2 1 6 1 6 1 0 0	4 4 3 5 3 2 1 1 6 1 0 0	948, 8496, 65520, 425484
2	2 2 5 1 3 1 6 1 6 1 0 0	3 5 4 4 6 4 2 1 6 1 0 0	894, 8802, 64572, 427236
3	6 4 4 1 4 1 6 1 6 1 0 0	3 6 2 6 1 2 2 1 6 1 0 0	936, 8436, 65580, 427704
4	2 6 2 3 5 1 6 1 6 1 0 0	5 3 3 4 4 2 1 1 6 1 0 0	882, 8592, 65544, 427086
5	5 6 5 4 5 1 6 1 6 1 0 0	2 1 3 5 1 5 1 1 6 1 0 0	774, 8706, 66204, 426204
6	1 4 2 2 1 2 6 1 6 1 0 0	3 3 5 6 3 4 2 1 6 1 0 0	948, 8466, 65520, 426306
7	4 5 3 4 4 2 6 1 6 1 0 0	1 3 5 1 2 1 2 1 6 1 0 0	936, 8982, 63516, 426750
8	1 6 4 6 4 3 6 1 6 1 0 0	2 1 6 3 2 6 2 1 6 1 0 0	966, 8502, 65148, 426792
9	1 3 3 1 1 3 6 1 6 1 0 0	5 2 2 3 2 4 2 1 6 1 0 0	966, 8700, 64500, 425730
10	4 6 1 6 3 4 6 1 6 1 0 0	5 1 6 3 6 2 2 1 6 1 0 0	846, 8796, 65448, 424134

3 Building-up construction for self-dual codes over finite chain rings

3.1 Finite chain rings

A finite commutative ring with identity $\neq 0$ is called a *chain ring* if its ideals are linearly ordered by inclusion. This means that it has a unique maximal ideal, i.e., that it is a local ring. Let R be a finite chain ring, \mathfrak{m} the unique maximal ideal of R , and γ the generator of the unique maximal ideal \mathfrak{m} . Then $\mathfrak{m} = \langle \gamma \rangle = R\gamma$, where $R\gamma = \langle \gamma \rangle = \{\beta\gamma \mid \beta \in R\}$. We have $R = \langle \gamma^0 \rangle \supseteq \langle \gamma^1 \rangle \supseteq \dots \supseteq \langle \gamma^i \rangle \supseteq \dots$. This chain cannot be infinite, since R is finite. Therefore, there exists a positive integer i such that $\langle \gamma^i \rangle = \{0\}$. Let e be the minimal number such that $\langle \gamma^e \rangle = \{0\}$. We call e the *nilpotency index* of γ .

Let C be a linear code over a finite chain ring R of length n . Then its generator matrix is equivalent to the following generator matrix G :

$$G = \begin{bmatrix} I_{k_0} & A_{0,1} & A_{0,2} & \cdots & A_{0,e-1} & A_{0,e} \\ 0 & \gamma I_{k_1} & \gamma A_{1,2} & \cdots & \gamma A_{1,e-1} & \gamma A_{1,e} \\ 0 & 0 & \gamma^2 I_{k_2} & \cdots & \gamma^2 A_{2,e-1} & \gamma^2 A_{2,e} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \cdots & \gamma^{e-1} I_{k_{e-1}} & \gamma^{e-1} A_{e-1,e} \end{bmatrix}.$$

Let $|R|$ denote the cardinality of R and R^* the set of all units in R . We know that R^* is a multiplicative group under the multiplicative operation of R . Let $\mathbb{F} = R/\mathfrak{m} = R/\langle \gamma \rangle$ be the residue field with characteristic p , where p is a prime number. This implies that there exist integers q and r such that $|\mathbb{F}| = q = p^r$, and $\mathbb{F}^* = \mathbb{F} - \{0\}$. This implies that $|\mathbb{F}^*| = p^r - 1$. See [35] for codes over chain rings.

The following theorem is the building-up construction for self-dual codes over a finite chain ring R with the property that there exist α and β in R^* such that $\alpha^2 + \beta^2 + 1 = 0$ in

R .

Proposition 3.1. *Let R be a finite chain ring. Suppose that there exist α and β in R^* such that $\alpha^2 + \beta^2 + 1 = 0$ in R . Let $G_0 = (\mathbf{r}_i)$ be a generator matrix (not necessarily in standard form) of a self-dual code \mathcal{C}_0 over R of length $2n$, where \mathbf{r}_i are the row vectors with $1 \leq i \leq k$ for some positive integer k . Let \mathbf{x}_1 and \mathbf{x}_2 be vectors in R^{2n} such that $\mathbf{x}_1 \cdot \mathbf{x}_2 = 0$ in R and $\mathbf{x}_i \cdot \mathbf{x}_i = -1$ in R for each $i = 1, 2$. For each i , $1 \leq i \leq k$, let $s_i := \mathbf{x}_1 \cdot \mathbf{r}_i$, $t_i := \mathbf{x}_2 \cdot \mathbf{r}_i$, and $\mathbf{y}_i := (-s_i, -t_i, -\alpha s_i - \beta t_i, -\beta s_i + \alpha t_i)$ be a vector of length 4. Then the following matrix*

$$G = \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & & & & \\ 0 & 1 & 0 & 0 & & & & \\ \hline & & \mathbf{y}_1 & & & \mathbf{x}_1 & & \\ & & \vdots & & & \mathbf{x}_2 & & \\ & & \mathbf{y}_k & & & \mathbf{r}_1 & & \\ & & & & & \vdots & & \\ & & & & & \mathbf{r}_k & & \end{array} \right]$$

generates a self-dual code \mathcal{C} over R of length $2n + 4$.

Proof. The proof is very similar to that of Proposition 2.2. It is straightforward to see that \mathcal{C} is self-orthogonal, so $\mathcal{C} \subseteq \mathcal{C}^\perp$. By the exactly same reasoning as the proof of Proposition 2.2, we can show that no linear combination of the first two rows of G (with scalars in R) is in the span of the bottom n rows of G . It thus follows that $|\mathcal{C}| = |R|^2 |\mathcal{C}_0|$. Since $|\mathcal{C}_0| = |R|^n$, we have $|\mathcal{C}| = |R|^{n+2}$. Furthermore, we have $|\mathcal{C}| |\mathcal{C}^\perp| = |R|^{2n+4}$, so $|\mathcal{C}| = |\mathcal{C}^\perp|$. As $\mathcal{C} \subseteq \mathcal{C}^\perp$ and $|\mathcal{C}| = |\mathcal{C}^\perp|$, we have $\mathcal{C} = \mathcal{C}^\perp$, that is, \mathcal{C} is self-dual. \square

The following proposition shows that the converse of Proposition 3.1 also holds for chain rings where there exist α and β in R^* such that $\alpha^2 + \beta^2 + 1 = 0$ in R . That is, every self-dual code over such a chain ring can be obtained by the method given in Proposition 3.1. In fact, the following result over chain rings is a general version of Proposition 2.4 over finite fields, and its proof requires the property of chain rings. Proposition 2.4 is certainly a corollary of Proposition 3.2, but the proof of Proposition 2.4 is simpler than that of Proposition 3.2; thus we treated the finite field case in Section 2 separately due to its simplicity.

Proposition 3.2. *Let R be a finite chain ring. Suppose that there exist α and β in R^* such that $\alpha^2 + \beta^2 + 1 = 0$ in R . Any self-dual code \mathcal{C} over R of length $2n$ with n even ≥ 4 and free rank ≥ 4 is obtained from some self-dual code \mathcal{C}_0 over R of length $2n - 4$ (up to permutation equivalence) by the construction method given in Proposition 3.1.*

Proof. It is sufficient to show that there exist vectors $\mathbf{x}_1, \mathbf{x}_2$ in R^{2n-4} and a self-dual code \mathcal{C}_0 over R of length $2n - 4$ whose extended code \mathcal{C}_1 (constructed by the method in Proposition 3.1) is equivalent to \mathcal{C} . Let G be a generator matrix of \mathcal{C} in a standard form as follows:

$$G := \left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & \mathbf{a}_1 \\ 0 & 1 & 0 & 0 & \mathbf{a}_2 \\ 0 & 0 & 1 & 0 & \mathbf{a}_3 \\ 0 & 0 & 0 & 1 & \mathbf{a}_4 \\ \hline 0 & 0 & 0 & 0 & \mathbf{a}_5 \\ \vdots & \vdots & \vdots & \vdots & \\ 0 & 0 & 0 & 0 & \mathbf{a}_k \end{array} \right].$$

Clearly \mathcal{C} also has the following generator matrix G' :

$$G' := \left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & \mathbf{a}_1 \\ 0 & 1 & 0 & 0 & \mathbf{a}_2 \\ 1 & 0 & \alpha & \beta & \mathbf{a}_1 + \alpha\mathbf{a}_3 + \beta\mathbf{a}_4 \\ 0 & 1 & \beta & -\alpha & \mathbf{a}_2 + \beta\mathbf{a}_3 - \alpha\mathbf{a}_4 \\ \hline 0 & 0 & 0 & 0 & \mathbf{a}_5 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \mathbf{a}_k \end{array} \right].$$

Deleting the first four columns and the first and second rows of G' produces the following $(k-2) \times (2n-4)$ matrix G_0 :

$$G_0 := \left[\begin{array}{c} \mathbf{a}_1 + \alpha\mathbf{a}_3 + \beta\mathbf{a}_4 \\ \mathbf{a}_2 + \beta\mathbf{a}_3 - \alpha\mathbf{a}_4 \\ \mathbf{a}_5 \\ \vdots \\ \mathbf{a}_k \end{array} \right].$$

We claim that G_0 is a generator matrix of some self-dual code \mathcal{C}_0 of length $2n-4$. First of all, we observe that G_0 generates a self-orthogonal code \mathcal{C}_0 ; this follows easily from the following facts: $\mathbf{a}_i \cdot \mathbf{a}_j = 0$ for $1 \leq i < j \leq k$, $\mathbf{a}_i \cdot \mathbf{a}_i = 0$ for $5 \leq i \leq k$, $\mathbf{a}_i \cdot \mathbf{a}_i = -1$ for $1 \leq i \leq 4$, and $\alpha^2 + \beta^2 + 1 = 0$ in R . Next we note that the R -span of the bottom $k-4$ rows of G has size $|R|^{n-4}$ as the first 4 rows of G have R -span size $|R|^4$. Thus the R -span of the bottom $k-4$ rows of G_0 also has size $|R|^{n-4}$. Hence to show that $|\mathcal{C}_0| = |R|^{n-2}$, we prove that (a) both vectors $\mathbf{v}_1 := \mathbf{a}_1 + \alpha\mathbf{a}_3 + \beta\mathbf{a}_4$ and $\mathbf{v}_2 := \mathbf{a}_2 + \beta\mathbf{a}_3 - \alpha\mathbf{a}_4$ give free rank 2 (that is, the R -span of $\{\mathbf{v}_1, \mathbf{v}_2\}$ has size $|R|^2$) and that (b) only the zero vector in the R -span of $\{\mathbf{v}_1, \mathbf{v}_2\}$ is in the R -span of $\{\mathbf{a}_5, \dots, \mathbf{a}_k\}$.

For the part (a), unlike the finite field case, showing that $\{\mathbf{v}_1, \mathbf{v}_2\}$ is linearly independent over R is insufficient since the R -span of $\{\mathbf{v}_1, \mathbf{v}_2\}$ does not necessarily give size $|R|^2$. Instead we show in detail that \mathbf{v}_1 and \mathbf{v}_2 give free rank 2 as follows. We first note that both vectors $\mathbf{v}_1, \mathbf{v}_2$ contain unit components. If not, i.e., \mathbf{v}_1 contains no unit components, then $\mathbf{v}_1 = \gamma\mathbf{w}$ for some \mathbf{w} in R^{2n-4} with γ the generator of the unique maximal ideal \mathfrak{m} of R ; so $\mathbf{a}_1 \cdot \mathbf{a}_3 = (-\alpha\mathbf{a}_3 - \beta\mathbf{a}_4 + \gamma\mathbf{w}) \cdot \mathbf{a}_3$. Thus we get $-\alpha = \gamma(\mathbf{w} \cdot \mathbf{a}_3)$, and this shows that a unit $-\alpha$ is contained in \mathfrak{m} , a contradiction. Similarly, it also holds for \mathbf{v}_2 . In fact, both

$\mathbf{v}_1, \mathbf{v}_2$ contain at least two unit components; otherwise, \mathbf{v}_1 has only one unit component, say u_1 . Then since $\mathbf{v}_1 \cdot \mathbf{v}_1 = 0$, we have $u_1^2 + \gamma z = 0$ for some z in R , which implies $u_1^2 \in \mathfrak{m}$, a contradiction. This is also true for \mathbf{v}_2 . Furthermore, we can show that $\mathbf{v}_1 \neq u\mathbf{v}_2$ for any u in R^* in exactly the same way as in Proposition 2.4. Hence, it follows that the R -span of $\{\mathbf{v}_1, \mathbf{v}_2\}$ is free of rank 2. For the part (b), suppose that $c_1\mathbf{v}_1 + c_2\mathbf{v}_2 = \sum_{i=5}^k b_i\mathbf{a}_i$ where $b_i \in R$ for $5 \leq i \leq k$. Then for $j = 1, 2$, $-c_j = (c_1\mathbf{v}_1 + c_2\mathbf{v}_2) \cdot \mathbf{a}_j$ but $(\sum_{i=5}^k b_i\mathbf{a}_i) \cdot \mathbf{a}_j = 0$. Hence $c_j = 0$ for $j = 1, 2$ as required.

Therefore we have $|\mathcal{C}_0| = |R|^{n-2}$, that is, \mathcal{C}_0 is self-dual. The rest of the proof is the same as that of Proposition 2.4. \square

3.2 Galois Rings

One of the important examples of chain rings is a Galois ring. In [31] we give the building-up method for self-dual codes over Galois rings $\text{GR}(p^m, r)$ in all the cases except the case $p \equiv 3 \pmod{4}$ with r odd. We complete the missing case by using Proposition 3.1 and Proposition 3.2 as follows.

Proposition 3.3. *The building-up method works over any Galois ring $\text{GR}(p^m, r)$ with p an odd prime. More precisely, if $p \equiv 1 \pmod{4}$, then the building-up method is given by [31, Proposition 3.3, 3.4], and if $p \equiv 3 \pmod{4}$, then the building-up method is given by Proposition 3.1, 3.2.*

Proof. It suffices to show it for the case $p \equiv 3 \pmod{4}$. By Propositions 3.1 and 3.2, we know that the building-up method works over Galois rings $\text{GR}(p^m, r)$ if there exist α and β in $\text{GR}(p^m, r)^*$ such that $\alpha^2 + \beta^2 + 1 = 0$ in $\text{GR}(p^m, r)$. In fact, we have $\mathbb{Z}_{p^m} \subseteq \text{GR}(p^m, r)$. It is therefore enough to show that when $p \equiv 3 \pmod{4}$, there exist α and β in $(\mathbb{Z}_{p^m})^*$ such that $\alpha^2 + \beta^2 + 1 = 0$ in \mathbb{Z}_{p^m} . If $p \equiv 3 \pmod{4}$, then by Lemma 2.1 there exist α and β in \mathbb{Z}_p^* such that $\alpha^2 + \beta^2 + 1 = 0$ in \mathbb{Z}_p . We notice that 2 and α are units in \mathbb{Z}_{p^i} for any positive integer i . From [9, Lemma 3.9], it follows that $x_m^2 + y_m^2 + 1 = 0$ in \mathbb{Z}_{p^m} for any integer $m \geq 1$, where x_m and y_m are defined recursively as follows: We first let

$$\begin{aligned} x_1 &= \alpha, \quad y_1 = \beta, \quad r_1 = (x_1^2 + y_1^2 + 1)/p, \\ \tilde{r}_1 &\equiv -\frac{r_1}{2\alpha} \pmod{p}, \quad \text{where } 0 \leq \tilde{r}_1 < p, \\ x_2 &= x_1 + \tilde{r}_1 p, \quad y_2 = \beta. \end{aligned}$$

An easy calculation shows that $x_2^2 + y_2^2 + 1 \equiv 0 \pmod{p^2}$ and $x_2, y_2 \in \mathbb{Z}_{p^2}^*$. Assuming that there exist $x_{i-1}, y_{i-1} \in \mathbb{Z}_{p^{i-1}}^*$ such that $x_{i-1}^2 + y_{i-1}^2 + 1 \equiv 0 \pmod{p^{i-1}}$ and $x_{i-1} \equiv \alpha \pmod{p}$, we recursively define $r_{i-1} = (x_{i-1}^2 + y_{i-1}^2 + 1)/p^{i-1}$, $\tilde{r}_{i-1} \equiv -\frac{r_{i-1}}{2\alpha} \pmod{p}$ where $0 \leq \tilde{r}_i < p$, $x_i = x_{i-1} + \tilde{r}_{i-1}p^{i-1}$, and $y_i = \beta$. A straightforward calculation shows that $x_i \equiv \alpha \pmod{p}$, $x_i^2 + y_i^2 + 1 \equiv 0 \pmod{p^i}$, and $x_i, y_i \in \mathbb{Z}_{p^i}^*$. In particular

$$x_m = \alpha + \tilde{r}_1 p + \tilde{r}_2 p^2 + \cdots + \tilde{r}_{m-1} p^{m-1}, \quad y_m = \beta,$$

and we have $x_m^2 + y_m^2 + 1 = 0$ in \mathbb{Z}_{p^m} . \square

3.3 Self-dual codes over \mathbb{Z}_9 and their lattices

In this section we consider self-dual codes over a Galois ring $R = \text{GR}(3^2, 1) = \mathbb{Z}_9$ and reconstruct optimal Type I lattices of dimensions 12, 16, 20, and 24 using Construction A, which is described below (see [3, 7, 11]).

Definition 3.4. (*Construction A*) Let m be any integer greater than 1. If C is a self-dual code of length n over \mathbb{Z}_m , then the lattice

$$\Lambda(C) = \frac{1}{\sqrt{m}} \{ \mathbf{x} = (x_1, \dots, x_n) \in \mathbb{Z}^n \mid (x_1 \pmod{m}, \dots, x_n \pmod{m}) \in C \}$$

is an n -dimensional unimodular lattice with the minimum norm $\mu = \min\{\frac{d_E(C)}{m}, m\}$, where $d_E(C)$ denotes the minimum Euclidean weight of C .

From Proposition 3.3 there exist α and β in R^* such that $\alpha^2 + \beta^2 + 1 = 0$ in R . We take $\alpha = 2$ and $\beta = 2$. For example, $\{(1, 0, 2, 2), (0, 1, 2, -2)\}$ generates a self-dual code \mathcal{C}_1 over \mathbb{Z}_9 of length 4 with minimum Hamming weight 3.

By using Proposition 3.1 starting from \mathcal{C}_1 with $\mathbf{x}_1 = (1, 3, 5, 0)$ and $\mathbf{x}_2 = (3, 8, 0, 4)$, we find the following generator matrix G_2 of the self-dual code \mathcal{C}_2 over \mathbb{Z}_9 of length 8 with minimum Hamming weight 3.

$$G_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 3 & 5 & 0 \\ 0 & 1 & 0 & 0 & 3 & 8 & 0 & 4 \\ 7 & 7 & 1 & 0 & 1 & 0 & 2 & 2 \\ 5 & 0 & 1 & 1 & 0 & 1 & 2 & 7 \end{bmatrix}.$$

Its Hamming weight enumerator is $W_2(x, y) = x^8 + 16x^5y^3 + 48x^4y^4 + 240x^3y^5 + 1072x^2y^6 + 2688xy^7 + 2496y^8$.

In what follows, we construct free self-dual codes over \mathbb{Z}_9 of lengths 12, 16, and 20 all with minimum Hamming weight 6. These codes can be regarded as codes over $GF(3)$ by taking each coordinate modulo 3. It is easy to see that the latter codes, called the *residue codes* $\text{Res}(\mathcal{C})$, are self-dual over $GF(3)$. In general, one can show that the residue code $\text{Res}(\mathcal{C})$ of a *free* self-dual code \mathcal{C} over \mathbb{Z}_9 is also self-dual over $GF(3)$ and that the minimum Hamming weight $d(\mathcal{C})$ is the same as that of $\text{Res}(\mathcal{C})$. (In fact, it is known [10, 35] that $d(\mathcal{C}) = d(\text{Tor}(\mathcal{C}))$ where $\text{Tor}(\mathcal{C}) = \{\mathbf{v} \pmod{3} \mid 3\mathbf{v} \in \mathcal{C}\}$. Since $\text{Tor}(\mathcal{C}) = \text{Res}(\mathcal{C})$ for a free self-dual code \mathcal{C} over \mathbb{Z}_9 , the claim follows.) Our self-dual codes over \mathbb{Z}_9 given below will attain the highest possible minimum Hamming weight 6 which free self-dual codes over \mathbb{Z}_9 of lengths 12, 16, and 20 can attain; it was known that the largest Hamming weight of self-dual codes over $GF(3)$ of lengths 12, 16, and 20 is 6 [26].

Applying Proposition 3.1 to G_2 , we obtain self-dual codes of length 12 with Hamming weight 6. We list eight inequivalent self-dual codes in Table 5, where the six entries of the right side of \mathbf{x}_1 and \mathbf{x}_2 respectively are displayed in the second column and in the third column, the fourth column gives the number A_6 of codewords with minimum weight 6, and the last column gives the minimum norm of the corresponding lattice. By Construction A, we obtain the unique optimal Type I lattice of dimension 12 [7, 11]. As far as we know,

only one self-dual code over \mathbb{Z}_9 of length 12 with Hamming weight 6 is obtained by lifting the extended ternary Golay $[12, 6, 6]$ linear code to a code over \mathbb{Z}_9 [5, 16], and this code has $A_6 = 264$, which shows that our codes in Table 5 are certainly new.

In particular, the first code in Table 5 has generator matrix given as follows:

$$G_3 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 4 & 5 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 7 & 0 & 1 \\ 0 & 4 & 8 & 1 & 1 & 0 & 0 & 0 & 1 & 3 & 5 & 0 \\ 7 & 6 & 8 & 2 & 0 & 1 & 0 & 0 & 3 & 8 & 0 & 4 \\ 2 & 3 & 1 & 7 & 7 & 7 & 1 & 0 & 1 & 0 & 2 & 2 \\ 6 & 0 & 3 & 3 & 5 & 0 & 1 & 1 & 0 & 1 & 2 & 7 \end{bmatrix}.$$

Similarly, using Proposition 3.1 with G_3 , we obtain many inequivalent self-dual codes of length 16 with Hamming weight 6 and $A_6 = 230 + 6t$ for $t = 0, 1, \dots, 19$. Table 6 presents twenty of them, where the eight entries of the right side of \mathbf{x}_1 and \mathbf{x}_2 respectively are displayed in the second and the third column. By Construction A, we obtain the unique optimal Type I lattice of dimension 16 [7, 11]. As an example, the self-dual code \mathcal{C}_4 (denoted by No. 1 in Table 6) over \mathbb{Z}_9 of length 16 with Hamming weight 6 has the following generator matrix G_4 :

$$G_4 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 4 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 7 & 2 & 7 & 2 & 0 & 1 & 0 & 0 \\ 8 & 6 & 1 & 4 & 1 & 0 & 0 & 0 & 0 & 0 & 4 & 5 & 1 & 1 & 1 & 0 \\ 3 & 2 & 1 & 2 & 0 & 1 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 7 & 0 & 1 \\ 4 & 8 & 6 & 1 & 0 & 4 & 8 & 1 & 1 & 0 & 0 & 0 & 1 & 3 & 5 & 0 \\ 2 & 8 & 2 & 6 & 7 & 6 & 8 & 2 & 0 & 1 & 0 & 0 & 3 & 8 & 0 & 4 \\ 5 & 2 & 5 & 6 & 2 & 3 & 1 & 7 & 7 & 7 & 1 & 0 & 1 & 0 & 2 & 2 \\ 5 & 0 & 1 & 1 & 6 & 0 & 3 & 3 & 5 & 0 & 1 & 1 & 0 & 1 & 2 & 7 \end{bmatrix}.$$

Using Proposition 3.1 with G_4 , we obtain many inequivalent self-dual codes of length 20 with Hamming weight 6 and distinct values of A_6 . In Table 7 we display ten such codes, where τ denotes the kissing number of the corresponding lattices $\Lambda(C)$. From the three distinct kissing numbers, we know that we have constructed at least three of the 12 inequivalent optimal Type I lattices of dimension 20 (see [7, Ch. 16] or [11]). It is interesting to note that in Table 7 the lattice $\Lambda(C)$ from the 10th code with $\tau = 120$ has $|\text{Aut}\Lambda(C)| = 31310311587840$ while the others with $\tau = 120$ have $|\text{Aut}\Lambda(C)| = 4299816960000$. Hence we have constructed at least four of the 12 inequivalent optimal Type I lattices of dimension 20. The first code in Table 7 has the generator matrix G_5 as follows:

Table 5: Self-dual codes of length 12 over $\text{GR}(3^2, 1) = \mathbb{Z}_9$ from G_2

Code No.	$\mathbf{x}_1 = (00x_3 \dots x_8)$	$\mathbf{x}_2 = (00x_3 \dots x_8)$	A_6	$\mu(\Lambda(C))$
1	4 5 1 1 1 0	2 2 2 7 0 1	516	2
2	4 5 1 1 1 0	8 6 5 4 1 1	552	2
3	4 5 1 1 1 0	5 3 2 7 1 1	444	2
4	4 5 1 1 1 0	8 3 8 7 1 1	480	2
5	4 5 1 1 1 0	2 5 5 4 3 1	588	2
6	4 5 1 1 1 0	2 2 8 6 4 1	408	2
7	4 5 1 1 1 0	3 5 5 5 7 1	624	2
8	5 5 1 1 1 0	0 8 7 2 5 8	660	2

$$G_5 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 4 & 4 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 6 & 6 & 2 & 3 & 1 & 1 & 1 & 1 & 0 & 0 \\ 4 & 4 & 7 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 4 & 1 & 1 & 1 & 0 & 0 & 0 \\ 5 & 6 & 4 & 7 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 7 & 2 & 7 & 2 & 0 & 1 & 0 & 0 \\ 7 & 7 & 1 & 0 & 8 & 6 & 1 & 4 & 1 & 0 & 0 & 0 & 0 & 4 & 5 & 1 & 1 & 1 & 0 \\ 5 & 5 & 2 & 0 & 3 & 2 & 1 & 2 & 0 & 1 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 7 & 0 & 1 \\ 1 & 3 & 8 & 5 & 4 & 8 & 6 & 1 & 0 & 4 & 8 & 1 & 1 & 0 & 0 & 0 & 1 & 3 & 5 & 0 \\ 2 & 7 & 0 & 8 & 2 & 8 & 2 & 6 & 7 & 6 & 8 & 2 & 0 & 1 & 0 & 0 & 3 & 8 & 0 & 4 \\ 3 & 5 & 7 & 5 & 5 & 2 & 5 & 6 & 2 & 3 & 1 & 7 & 7 & 7 & 1 & 0 & 1 & 0 & 2 & 2 \\ 7 & 5 & 6 & 4 & 5 & 0 & 1 & 1 & 6 & 0 & 3 & 3 & 5 & 0 & 1 & 1 & 0 & 1 & 2 & 7 \end{bmatrix}.$$

Applying Proposition 3.1 to G_5 produces several inequivalent self-dual codes of length 24 with Hamming weight 6. Their corresponding lattices $\Lambda(C)$ have minimum norm 3, and thus each must be the *odd Leech lattice*. We list three codes in Table 8 where the twelve entries of the right side of \mathbf{x}_1 and \mathbf{x}_2 respectively are written in the second and the third column.

4 Conclusion

We have completed the open cases of the building-up construction for self-dual codes over $GF(q)$ with $q \equiv 3 \pmod{4}$ and over \mathbb{Z}_{p^m} and Galois rings $GR(p^m, r)$ with $p \equiv 3 \pmod{4}$. We have also generalized the building-up construction for self-dual codes to codes over finite chain rings. As a result, the building-up construction works over any finite fields $GF(q)$, finite rings \mathbb{Z}_{p^m} , and Galois rings $GR(p^m, r)$.

We have seen that the building-up construction is a very efficient way of finding many self-dual codes of reasonable lengths. In particular, we construct 945 new extremal self-dual ternary [32, 16, 9] codes with trivial automorphism groups, and we obtain new optimal self-dual [16, 8, 7] codes over $GF(7)$ and new self-dual codes over $GF(7)$ with the best known parameters [24, 12, 9]. We also construct many new self-dual codes over \mathbb{Z}_9 of lengths 12, 16, 20 all with minimum Hamming weight 6, which is the best possible minimum Hamming weight

Table 6: Self-dual codes of length 16 over $\text{GR}(3^2, 1) = \mathbb{Z}_9$ from G_3

Code No.	$\mathbf{x}_1 = (0000x_5 \dots x_{12})$	$\mathbf{x}_2 = (0000x_5 \dots x_{12})$	A_6	$\mu(\Lambda(C))$
1	4 4 1 1 1 0 0 0	7 2 7 2 0 1 0 0	266	2
2	4 4 1 1 1 0 0 0	7 4 8 2 0 1 0 0	278	2
3	4 4 1 1 1 0 0 0	1 8 5 4 0 1 0 0	248	2
4	4 4 1 1 1 0 0 0	4 8 1 5 0 1 0 0	254	2
5	4 4 1 1 1 0 0 0	1 8 4 5 0 1 0 0	260	2
6	4 4 1 1 1 0 0 0	1 1 5 5 0 1 0 0	284	2
7	4 4 1 1 1 0 0 0	7 4 2 8 0 1 0 0	296	2
8	4 4 1 1 1 0 0 0	1 5 4 8 0 1 0 0	338	2
9	4 4 1 1 1 0 0 0	8 1 2 6 1 1 0 0	272	2
10	4 4 1 1 1 0 0 0	7 5 3 1 2 1 0 0	242	2
11	4 4 1 1 1 0 0 0	8 2 1 1 3 1 0 0	302	2
12	4 4 1 1 1 0 0 0	2 8 1 1 3 1 0 0	290	2
13	4 4 1 1 1 0 0 0	2 2 4 1 6 1 0 0	326	2
14	4 4 1 1 1 0 0 0	1 7 2 5 6 1 0 0	230	2
15	4 4 1 1 1 0 0 0	5 4 7 2 0 2 0 0	308	2
16	4 4 1 1 1 0 0 0	8 7 8 4 0 2 0 0	314	2
17	4 4 1 1 1 0 0 0	1 8 4 3 2 2 0 0	320	2
18	4 4 1 1 1 0 0 0	7 2 4 0 5 2 0 0	332	2
19	4 4 1 1 1 0 0 0	4 1 2 8 6 2 0 0	344	2
20	4 4 1 1 1 0 0 0	7 2 3 7 8 7 0 0	236	2

Table 7: Self-dual codes of length 20 over $\text{GR}(3^2, 1) = \mathbb{Z}_9$ from G_4

#	$\mathbf{x}_1 = (0 \dots 0x_7 \dots x_{16})$	$\mathbf{x}_2 = (0 \dots 0x_7 \dots x_{16})$	A_6, A_7	$\mu(\Lambda(C))$	τ
1	4 4 4 1 1 1 1 1 0 0	6 6 2 3 1 1 1 1 0 0	138, 138	2	152
2	4 4 4 1 1 1 1 1 0 0	4 4 4 1 1 1 1 1 0 0	138, 60	2	152
3	4 4 4 1 1 1 1 1 0 0	2 5 2 5 1 1 1 1 0 0	138, 132	2	152
4	4 4 4 1 1 1 1 1 0 0	8 5 5 5 1 1 1 1 0 0	138, 36	2	120
5	4 4 4 1 1 1 1 1 0 0	5 8 5 5 1 1 1 1 0 0	138, 90	2	120
6	4 4 4 1 1 1 1 1 0 0	5 5 8 5 1 1 1 1 0 0	132, 48	2	120
7	4 4 4 1 1 1 1 1 0 0	6 2 3 6 1 1 1 1 0 0	144, 36	2	120
8	4 4 4 1 1 1 1 1 0 0	5 7 2 2 2 1 1 1 0 0	120, 30	2	152
9	4 4 4 1 1 1 1 1 0 0	2 6 6 1 3 1 1 1 0 0	126, 42	2	184
10	4 4 4 1 1 1 1 1 0 0	6 5 4 6 3 1 1 1 0 0	126, 36	2	120

Table 8: Self-dual codes of length 24 over $\text{GR}(3^2, 1) = \mathbb{Z}_9$ from G_5

Code No.	$\mathbf{x}_1 = (0 \cdots 0x_9 \dots x_{24})$	$\mathbf{x}_2 = (0 \dots 0x_9 \dots x_{24})$	A_6	$\mu(\Lambda(C))$
1	4 3 2 1 1 1 1 1 0 0 0	7 7 1 4 7 2 6 1 1 0 0 0	48	3
2	4 3 2 1 1 1 1 1 0 0 0	2 1 2 4 7 2 6 1 1 0 0 0	40	3
3	4 3 2 1 1 1 1 1 0 0 0	4 7 6 2 2 1 7 1 1 0 0 0	32	3

that free self-dual codes over \mathbb{Z}_9 of these lengths can attain. Furthermore, from the constructed codes over \mathbb{Z}_9 , we are able to reconstruct optimal Type I lattices of dimensions 12, 16, 20, and 24 using Construction A. We conclude that our building-up construction can provide a nice way of constructing optimal Type I lattices as well as self-dual codes.

Acknowledgment

The authors would like to thank Dr. Thomas Feulner for his comments. J.-L. Kim was partially supported by the Project Completion Grant (year 2011-2012) at the University of Louisville.

References

- [1] C. Aguilar Melchor and P. Gaborit, “On the classification of extremal [36, 18, 8] binary self-dual codes,” *IEEE Transactions on Information Theory*, vol. 54, no 10, pp. 4743–4750, 2008.
- [2] C. Aguilar-Melchor, P. Gaborit, J.-L. Kim, L. Sok, and P. Solé, Classification of extremal and s -extremal binary self-dual codes of length 38, to appear in *IEEE Trans. Inform. Theory*.
- [3] E. Bannai, S.T. Dougherty, M. Harada, M. Oura, *Type II codes, even unimodular lattices, and invariant rings*, *IEEE Trans. Inform. Theory* vol. **45** (1999), 1194–1205.
- [4] R.A. Brualdi, V. Pless, *Weight enumerators of self-dual codes*, *IEEE Trans. Inform. Theory* vol. **37** (1991), 1222–1225.
- [5] A.R. Calderbank, N.J.A. Sloane, *The ternary Golay code, the integers mod 9, and the Coxeter-Todd lattice*, *IEEE Inform. Theory* vol. **42** no.2 (1996), 636.
- [6] J. Cannon, C. Playoust, “An Introduction to Magma,” University of Sydney, Sydney, Australia, 1994.
- [7] J.H. Conway, N.J.A. Sloane, “Sphere Packing, Lattices and Groups,” 3rd Ed., Springer-Verlag, New York, 1999.

- [8] S.T. Dougherty, *Shadow codes and weight enumerators*, IEEE Trans. Inform. Theory vol. **41** no.3 (1995), 762–768.
- [9] S.T. Dougherty, Y. Park, *Codes over the p -adic integer*, Des. Codes Cryptogr. vol. **39** no 1 (2006), 65–80.
- [10] S.T. Dougherty, J.-L. Kim, H. Liu, *Constructions of self-dual codes over chain rings*, preprint, 2008.
- [11] P. Gaborit, *Construction of new extremal unimodular lattices*, European J. Combin. vol. **25** (2004), 549–564.
- [12] T.A. Gulliver, M. Harada, *New optimal self-dual codes over $GF(7)$* , Graphs Combin. vol. **15** (1999), 175–186.
- [13] T.A. Gulliver, M. Harada, H. Miyabayashi, *Double circulant and quasi-twisted self-dual codes over \mathbb{F}_5 and \mathbb{F}_7* , Adv. Math. Commun. **1** No. 2 (2007), 223–238.
- [14] T.A. Gulliver, J.-L. Kim, Y. Lee, *New MDS or near-MDS self-dual codes*, IEEE Trans. Inform. Theory, **54** no.9 (2008), 4354–4360.
- [15] F.Q. Gouvêa, “ P -adic numbers: an introduction,” Springer-Verlag, New York-Berlin, 1993.
- [16] M. Greferath, E. Viterbo, *On \mathbb{Z}_4 - and \mathbb{Z}_9 -linear lifts of the Golay codes*, IEEE Trans. Inform. Theory, **45** no.7 (1999), 2524–2527.
- [17] M. Harada, personal communication on April 25, 2009.
- [18] M. Harada, *The existence of a self-dual $[70, 35, 12]$ code and formally self-dual codes*, Finite Fields Appl. **3** (1997), 131–139.
- [19] M. Harada, *New extremal ternary self-dual codes*, Austral. J. Combin. **17** (1998), 133–145.
- [20] M. Harada, *An extremal ternary self-dual $[28, 14, 9]$ code with a trivial automorphism group*, Discrete Math. **239** (2001), 121–125.
- [21] M. Harada, W. Holzmann, H. Kharaghani, M. Khorvash, *Extremal ternary self-dual codes constructed from negacirculant matrices*, Graphs Combin. **23** (2007), 401–417.
- [22] M. Harada, H. Kharaghani, *Orthogonal designs, self-dual codes, and Leech lattice*, J. Combin. Designs, **13** (2005), 184–194.
- [23] M. Harada, A. Munemasa, B. Venkov, *Classification of ternary extremal self-dual codes of length 28*, to appear in Math. Comp.
- [24] M. Harada, P.R.J. Östergård, *Self-dual and maximal self-orthogonal codes over \mathbb{F}_7* , Discrete Math. **256** (2002), 471–477.

- [25] W.C. Huffman, *On extremal self-dual ternary codes of lengths 28 to 40*, IEEE Trans. Inform. Theory, **38** (1992), 139–400.
- [26] W.C. Huffman, *On the classification and enumeration of self-dual codes*, Finite Fields Appl. **11** (2005), 451–490.
- [27] W.C. Huffman, V. S. Pless, “Fundamentals of Error-correcting Codes,” Cambridge: Cambridge University Press, 2003.
- [28] K.F. Ireland, M. Rosen, “A classical introduction to modern number theory,” Springer-Verlag, New York-Berlin, 1982.
- [29] J.-L. Kim, *New extremal self-dual codes of lengths 36, 38 and 58*, IEEE Trans. Inform. Theory, **47** (2001), 386–393.
- [30] J.-L. Kim, Y. Lee, *Euclidean and Hermitian self-dual MDS codes over large finite fields*, J. Combin. Theory Ser. A, **105** (2004), 79–95.
- [31] J.-L. Kim, Y. Lee, *Construction of MDS Self-dual codes over Galois rings*, Des. Codes Cryptogr., **45** no. 2 (2007), 247–258.
- [32] H. Koch, *On self-dual doubly-even codes of length 32*, J. Combin. Theory Ser. A, **51** (1989), 63–76.
- [33] H. Lee, Y. Lee, *Construction of self-dual codes over finite rings \mathbb{Z}_{p^m}* , J. Combin. Theory Ser. A, **115** (2008), 407–422.
- [34] J. S. Leon, V. Pless, N. J. A. Sloane, *On ternary self-dual codes of length 24*, IEEE Trans. Inform. Theory, **27** no. 2 (1981), 176–180.
- [35] G. H. Norton, A. Sălăgean, *On the Hamming distance of linear codes over a finite chain ring*, IEEE Trans. Inform. Theory, **46**, no. 3 (2000), 1060–1067.
- [36] V. Pless, *On the classification and enumeration of self-dual codes*, J. Combin. Theory Ser. A, **18** no. 3 (1975), 313–335.
- [37] V. Pless, *Symmetry codes over $GF(3)$ and new five-designs*, J. Combin. Theory Ser. A, **12** no. 1 (1972), 119–142.
- [38] V. Pless, V. Tonchev, *Self-dual codes over $GF(7)$* , IEEE Trans. Inform. Theory **33** no. 5 (1987), 723–727.
- [39] E. Rains, N.J.A. Sloane, *Self-dual codes*, in: V.S. Pless, W.C. Huffman (Eds.), “Handbook of Coding Theory,” Elsevier, Amsterdam. The Netherlands, 1998.